サイバー・セキュリティに対する ファーウェイの視点と取り組み

エンド・ツー・エンドのサイバー・セキュリティ保証のために テクノロジー・ベンダーに確認すべき 100 の質問

ジョン・サフォーク

ファーウェイ・テクノロジーズ
上級副社長
グローバル・サイバー・セキュリティ責任者

2014 年 12 月

HUAWEI

謝　辞

本資料の作成にあたり多大なご助力をいただいた次の方々に謝意を表します。劉海軍、南建峰、王唯践、デビッド・フランシス（David Francis）、アンディ・パーディ（Andy Purdy）、デバブラタ・ナヤク（Debabrata Nayak）、ピーター・ロッシ（Peter Rossi）、アンディ・ホプキンズ（Andy Hopkins）、羅明、李花蘭、ワウト・ヴァン・ウェイク（Wout van Wijk）、ウィリアム・プラマー（William Plummer）、ルドビク・プティ（Ludovic Petit）、ウルフ・フェーガー（Ulf Feger）、牟徳俊、楊光磊 各氏。また、ここに名前を記すことができなかった方々にも、深く感謝します。

ジョン・サフォーク

目　次

1. 要　旨 1
2. はじめに 2
3. 質問リスト作成の背景 4
4. 強力なサイバー・セキュリティ・プログラムを設計するために考慮すべき質問と課題 5
4.1 戦略、ガバナンス、統制 6
4.2 標準とプロセス 8
4.3 法律と規制 9
4.4 人　材 10
4.5 研究開発 12
4.6 検証：先入観を持たず、誰も盲信せず、すべてを確認する 16
4.7 サードパーティ・サプライヤーの管理 18
4.8 製　造 20
4.9 安全なサービス・デリバリー 22
4.10 問題、障害、脆弱性の解決 24
4.11 監　査 25
5. ファーウェイについて 26

1 要　旨

2013 年 10 月に発行された当社の提言レポート『サイバー・セキュリティをファーウェイの DNA に――統合プロセス、指針、標準[1]』において、ファーウェイはエンド・ツー・エンドのサイバー・セキュリティ・プロセスに対する当社の包括的アプローチについて詳しく述べました。その中でお伝えしたとおり、今回の提言レポートではサイバー・セキュリティに関してお客様から多く寄せられる質問の上位 100 項目を文書にまとめました。これは、サイバー・セキュリティに対するアプローチに関して誰もがテクノロジー・ベンダーに聞いておきたい質問をリストアップしたものです。本提言レポートでは、テクノロジーを購入する際にベンダーに質問すべきこれら 100 項目の質問を詳説します。

その目的は、ファーウェイに寄せられた質問と、さまざまな「標準」やベスト・プラクティスに対する独自の評価に基づいて、購入者が入札時にベンダーのサイバー・セキュリティに関する能力を体系的に分析できるよう提言することです。

この質問リストを作成するにあたっては、さまざまなソースを参照しました。

- 第一に、お客様の声に熱心に耳を傾けました。お客様の問題や懸念は何か。お客様は何を心配されているか。お客様自身やその業界、あるいはその国の要件はどのようなものか。
- 大規模な通信インフラからクラウド・コンピューティング、さらには法人向けソリューションやコンシューマー・ソリューションに至るまで、あらゆる分野にまたがる ICT 業界のグローバル・リーダーとして、当社は 15 万人に及ぶ従業員、科学者、エンジニアの豊富な知識を有しています。リストの作成においても、こうした従業員の知識と熱意が活かされています。
- また、1,200 を超える「標準」、記事、ベスト・プラクティスを参照し、一貫性の確保に努めました。

当社は、多くの国において、サイバー・セキュリティに関する法的要件や業界要件が増大していることを認識しています。実際に、政府機関や規制当局が、サイバー・セキュリティに関する説明責任やそれを果たさなかった場合の法的責任を、国の基幹インフラのプロバイダーや、コンピューターや IT サービスのプロバイダーに転嫁する例も出てきています。ますます多くの企業が、サイバー・セキュリティに対してどのような取り組みを行っているか、取引のあるテクノロジー・ベンダーやサービス・プロバイダーについてどのような分析と評価を行ったのかを、詳細に説明せざるを得なくなるでしょう。

サービス・プロバイダーが、「知りませんでした」「優良なベンダーだと思っていました」と言って済まされる時代は、急速に過ぎ去りつつあります。テクノロジーの購入者が、一貫性のない質問でさまざまなサプライヤーを評価する時代は、もはや終わろうとしています。グローバルに絡み合った世界では、脅威はどこからでも生じる可能性があり、そして実際に生じているのです。この上位 100 項目の質問は、サプライヤーのサイバー・セキュリティに関する能力を評価する際に、自らのリスクを軽減するための第一歩となります。質の高いセキュリティ保証への要求がより厳しくなり、より一貫性を増すことにより ICT ベンダーはセキュリティへの投資を強化し、セキュリティの標準を引き上げるようになると私たちは確信しています。

本提言レポートの大部分は、ファーウェイが独自の調査に基づいて、テクノロジー・ベンダーを選定する際に考慮すべきであると考える 100 項目の質問の詳細な説明に充てられています。これらの項目は、「戦略、ガバナンス、統制」「標準とプロセス」「法律と規制」「人材」「研究開発」「検証」「サードパーティ・サプライヤーの管理」「製造」「安全なサービス・デリバリー」「問題、障害、脆弱性の解決」「監査」というセクションに分類されています。

[1] http://www.huawei.com/ilink/jp/download/HW_310660

各セクションにおいて、テクノロジー・ベンダーに質問すべき複数の要件を詳述します。さらに、各項目がなぜ重要となり得るのかについても論拠を示します。これらの質問の中には、内部監査人はどのようなことに注目するのか、自社のガバナンスにおいて何を考慮する必要があるのか、取締役会や監査委員会はどのようなことを質問するのかなど、読者の皆様の組織に関する有益な情報が得られるものもあるでしょう。

最後に、本レポートでは標準化団体に対してもいくつかの提言をしています。

- 第一に、異なる標準間における重複を削減するよう協力しあうべきです。
- 第二に、さまざまな標準を一貫した構成要素に基づくものになるよう再構成すべきです。例えば、「ガバナンスと管理」という構成要素は、これを必要とするすべての標準において同一であるべきであり、数多くの標準ごとに少しずつ異なるモジュールであってはなりません。
- 第三に、可能なかぎり、投入リソースや作業の定義よりも、成果の測定に重点を置くべきです。

当社としては、多くの企業、政策アドバイザー、ベンダー、技術の購入者の皆様に、今回の提言レポートを「バージョン 1.0」として改善点をご提案いただきたいと考えています。そのため、国際的シンクタンクである EWI（EastWest Institute）が、本レポートをより詳細なバージョンに改訂するプロジェクトの指揮を執ってくれることになりました。本レポートで提言するコンセプトが、テクノロジーの購入時に考慮すべき事項として定着し、ICT 業界が製品とサービスのセキュリティ設計、開発、実装を進歩させる一助となることを願っています。

2　はじめに

2013 年 10 月に発行された当社の提言レポート『サイバー・セキュリティをファーウェイの DNA に――統合プロセス、指針、標準[2]』において、ファーウェイはエンド・ツー・エンドのサイバー・セキュリティ・プロセスに対する当社の包括的アプローチについて詳しく述べました。その中でお伝えしたとおり、今回の提言レポートではサイバー・セキュリティに関してお客様から多く寄せられる質問の上位 100 項目を文書にまとめました。これは、サイバー・セキュリティに対するアプローチに関して誰もがテクノロジー・ベンダーに聞いておきたい質問をリストアップしたものです。

当社ではこのリストを「逆 RFI（Request For Information：情報提供依頼書）」と呼んでいます。つまりこれは、お客様が購入を考えているベンダーに対して満たしているかどうかを聞くべきサイバー・セキュリティ要件のリストなのです。「逆」というのは、ここでは通常の情報提供依頼プロセスが逆転し、ベンダーである当社がお客様に、サイバー・セキュリティにどのように対処しているかを問い合わせるよう促しているということです。

この提言レポート第 3 版には、上位 100 項目の質問と、そのリストを作成するために私たちが取ったアプローチを記しています。

ではまず、なぜサイバー・セキュリティの国際的な標準、規範、慣行を策定、合意、実施することがこれほど困難なのかという議論から始めましょう。それを実現することによって得られる見返りが、そのための労力に見合うほど十分なものではないからでしょうか。サイバー犯罪によって生じるとされている損害の大きさを見れば、これが間違っていることは明らかです。では、この問題が産業界や政界が取り組むべき課題とみなされていないからでしょうか。サイバー犯罪に関する国際的な政府会議の開催件数や、データの漏洩、知的財産の損失、サービス妨害攻撃によるオンライン・サービスの中断などに関する報道の多さを考えれば、これも間違っています。

[2] http://www.huawei.com/ilink/jp/download/HW_310660

おそらくその理由は、課題の規模があまりに大きすぎてどこから手をつけたらいいのかわからないこと、そして「標準」「ベスト・プラクティス」「ガイダンス」に対してあまりに多くの見方がありすぎることでしょう。前回の提言レポートで「標準化の問題は、標準が標準ではないことだ」と明言したとおり、これが大きな要因だと当社は考えます。また、既存の標準は、企業や政府機関、また場合によってはエンド・ユーザーに焦点を当てているものがほとんどで、ハードウェアやソフトウェアの生産者、すなわちベンダーに本気で焦点を当てるものは、あったとしてもごくわずかです。

テクノロジーの幅広さを考えると、私たちが「1 つの標準」にたどり着くことは現実的には不可能でしょう。私たちにできるのは、多数の標準、規約、ベスト・プラクティスの中で（おそらくは異なる言い回しを使って）文書化されていることが多い主要な要件に注目し、そうした要件をベンダー各社が共同で行うべき取り組みに当てはめ、自分たちの製品のセキュリティを向上させていくことです。

この提言レポートでは、サイバー・セキュリティに関して当社がお客様やその他のステークホルダーから最も頻繁に尋ねられる、技術以外の質問について詳しく説明します。ここで言う「最も頻繁に」というのは、最も多くの会話やレビュー、あるいはフォローアップの質問につながっているということでもあります。こうした質問に若干の修正を加えて一般化したうえで、このリストを作成しました。また、米国での機密暴露といった最近の問題を反映していくつかの質問を追加するとともに、セクションごとのまとまりを出すために補足の質問を挿入しました。

当社は会社全体で知識を継続的に強化していく努力の一環としてこれらの質問を提起し、サイバー・セキュリティの分野で「良いものとはかくあるべき」という評価に対して現在続けられている議論と取り組みに貢献することを目指します。

リストの作成にあたっては、各質問に優先順位をつけたり、特定の枠組みや方法論にはめ込んだりはしていません。基本的には、ファーウェイの中核プロセスのそれぞれに大まかに関連した質問をまとめるという構成になっています。

このリストはその性質上、あらゆる業界にとって包括的となり得るものではなく、またすべての法律や技術標準をカバーするものでもありません。それはこのリストの目的ではありません。このリストの目的は、購入者が入札の際にベンダーのサイバー・セキュリティに関する能力を体系的に分析し、その情報を活用して RFI や RFP（Request for Proposal：提案依頼書）の質を高めて、短期的および長期的な技術的ニーズを満たす最良のベンダーを見つけられるよう、ファーウェイに寄せられた質問と、「標準」やベスト・プラクティスに対する独自の評価に基づいて提言をすることです。

質の高いセキュリティ保証に対する購入者の要求がより厳しくなり、より一貫性を増すことにより、ICT ベンダーはセキュリティへの投資を強化し、セキュリティの標準を引き上げるようになると当社は確信しています。

私たちが一丸となって技術関連の製品やサービスにおけるセキュリティ面の考慮の質を高めれば、ICT の利用を通じて人々の生活を豊かにするためにさらに多くの貢献ができるのです。

3　質問リスト作成の背景

この質問リストを作成するにあたっては、さまざまなソースを参照しました。

- 第一に、お客様の声に熱心に耳を傾けました。お客様の問題や懸念は何か。お客様は何を心配されているか。お客様自身やその業界、あるいはその国の要件はどのようなものか。このような話をお客様からうかがうにあたり、当社はありがたいことに中国･深圳の本社キャンパスに何千人ものお客様にお越しいただき、ファーウェイの価値、能力、指針およびアプローチを実際に見ていただいています。こうした機会から、多くの質問や見解を得ることができました。ご意見を共有してくださったお客様に深く感謝しております。

- 大規模な通信インフラからクラウド・コンピューティング、さらには法人向けソリューションやコンシューマー・ソリューションに至るまで、あらゆる分野にまたがる ICT 業界のグローバル・リーダーとして、当社は 15 万人に及ぶ従業員、科学者、エンジニアの豊富な知識を有しています。リストの作成においても、こうした従業員の知識と熱意が活かされています。

- ファーウェイは一企業として、主流の国際標準への対応に熱心に取り組んでおり、そうした標準の策定にも積極的に貢献しています。2013 年末までにファーウェイは、3GPP（Third Generation Partnership Project：第 3 世代移動体通信システム標準化プロジェクト）、IETF（Internet Engineering Task Force：インターネット・エンジニアリング・タスク・フォース）、ITU（International Telecommunication Union：国際電気通信連合）、OMA（Open Mobile Alliance：オープン・モバイル・アライアンス）、ETSI（European Telecommunications Standards Institute：欧州電気通信標準化機構）、TMF（Tele Management Forum：テレマネジメント･フォーラム）、ATIS（Association of Technical Information Services:技術情報サービス協会）、オープン・グループなど、170 を超える業界標準化団体に参加しています。当社はこれまでにこれらの団体に累計 5,000 件を超える提案書を提出しており、現在 185 を超える役職に就いて、国際標準に対する合意形成の推進をサポートしています。標準とフレームワークに関して、当社は最近設置された NIST(National Institute of Standards and Technology：米国標準技術局）の立ち上げに貢献したほか、ISO27001 の強化をサポートするとともに、ITU と 3GPP の活動にも積極的に参画しています。この質問リストを作成するにあたり、こうした取り組みに関連する資料の多くを参考にしました。

- また、1,200 を超える「標準」、記事、ベスト・プラクティスを参照し、一貫性の確保に努めました。

当社はこの質問リストをできるだけ多くの方々に参考資料として利用していただきたいと願っていますが、これさえあれば誰でも容易にベンダーの能力を判断できるという包括的なものにすることは意図していません。質問をすることは簡単ですが、回答を理解して、それが正確で実証や検証が可能なものであるかどうかを確実に見極めるためのスキルも必要とされるのです。

ここで、標準化団体に対していくつかの提言をさせていただきます。

- 第一に、異なる標準間における重複を削減するよう協力しあうべきです。

- 第二に、さまざまな標準を一貫した構成要素に基づくものになるよう再構成すべきです。例えば、「ガバナンスと統制」という構成要素は、これを必要とするすべての標準において同一であるべきであり、数多くの標準ごとに少しずつ異なるモジュールであってはなりません。

- 第三に、可能なかぎり、投入リソースや作業の定義よりも、成果の測定に重点を置くべきです。

当社としては、将来的に皆様からのご意見を反映した改訂版を作成できるように、本レポートで追加、削除、あるいは修正すべき点に関するフィードバックをいただければ幸いです。

4　強力なサイバー・セキュリティ・プログラムを設計するために考慮すべき質問と課題

当社は、多くの国において、サイバー・セキュリティに関する法的要件や業界要件が増大していることを認識しています。実際に、政府機関や規制当局が、サイバー・セキュリティに関する説明責任や問題が起きた場合の法的責任を、国の基幹インフラのプロバイダーや、コンピューターや IT サービスのプロバイダーに転嫁する例も出てきています。これはプロバイダーにとって苦しい状況です。例えば、大量のデータ損失やサービスの損失が発生した場合、おそらく政府機関や規制当局はそれがセキュリティの問題に起因する事象であるとの想定のもと、サービス・プロバイダーにサイバー・セキュリティに対するアプローチについて尋ねるはずです。ますます多くの企業が、サイバー・セキュリティに対してどのような取り組みを行っているか、取引のあるテクノロジー・ベンダーやサービス・プロバイダーについてどのような分析と評価を行ったのかを、詳細に説明せざるを得なくなるでしょう。広義のサイバー・セキュリティは、法律から製造まで、サービスから人材まで、ガバナンスから研究開発までを含む非常に複雑なものだという事実が、状況をさらに難しくしています。世界中でそれほど広く深い知識を持っている人はほとんどいないため、質問すべき事柄や探すべきエビデンスが何なのかを把握できる人もほとんどいないのです。

サービス・プロバイダーが、「知りませんでした」「優良なベンダーだと思っていました」と言って済まされる時代は、急速に過ぎ去りつつあります。テクノロジーの購入者が、一貫性のない質問でさまざまなサプライヤーを評価する時代は、もはや終わろうとしています。グローバルに絡み合った世界では、脅威はどこからでも生じる可能性があり、そして実際に生じているのです。この上位 100 項目の質問は、サプライヤーのサイバー・セキュリティに関する能力を評価する際に、自らのリスクを軽減するための第一歩となります。

本項では、ベンダーのセキュリティ能力について検討する際に考慮すべきだと当社が考える上位 100 項目の要件を挙げます。ただし、そのすべてが常に当てはまるわけではありませんし、組織のあらゆるレベルに適用できるわけでもありません。さらに、あらゆる製品やサービスの購入時に適用できるわけでもありません。このリストを通じて、ベンダーを選ぶ際に考慮すべき点についての理解をさらに深めていただき、各社独自の要件をこのリストの中の質問のいくつかによって補うことで、すべてのテクノロジー・ベンダーがセキュリティの保証にいっそう注力するようになれば幸いです。

質問は、2013 年 10 月に発行したファーウェイの提言レポート第 2 版とおおむね同じセクションに分けられています。第 2 版のレポートでは、サイバー・セキュリティに対するファーウェイのアプローチを包括的に示しました。

上位 100 項目の質問を読んでいただくと、一部の質問は統合できるのではないかと思われるかもしれません。これについてはよく熟考しましたが、最終的には質問をできるだけ具体的にしておくよう努めました。統合すればするほど、焦点がぼやけるリスクが高くなるからです。また一部の質問は、フォローアップの質問がライフサイクルやプロセスの次の段階に関わるものになっていて、質問の内容が少し異なっている場合もあります。本レポートの最大の目的はすべてのテクノロジー・ベンダーにおけるセキュリティへの配慮の質を高めることですので、こうした質問の詳細については必要に応じて自由に変更していただければと思います。

4.1 戦略、ガバナンス、統制

取締役や幹部社員がサイバー・セキュリティを優先事項とみなさなければ、一般社員も優先事項とはみなしません。サイバー・セキュリティを企業の組織構造、ガバナンス、内部統制の枠組みに組み込むことが、優れたサイバー・セキュリティの設計・開発・提供の第一歩となります。

要件	さらなる考慮事項
1. ベンダーには、情報やサイバー・セキュリティに関するリスク管理に対する正式な戦略やアプローチがありますか。	• 戦略がなければ、投資やリソースが割り当てられる可能性は低いです。 • 組織は、サイバー・セキュリティが組織の業務運営（ミッション、役割、イメージ、評判を含む）、資産、個人に対してどのようなリスクを持っているかを理解している必要があります。 • 戦略の欠如は、見通しの立たない成り行き任せの結果と、品質やセキュリティの一貫性および再現性の欠如につながります。 • たとえ戦略があっても効果的なアプローチがなければ、その戦略は単なる絵空事になります。
2. ベンダーの戦略には、適切なガバナンス、組織設計、指針、手順が整備されていますか。また、サイバー・セキュリティに関する状況や要件の変化にあわせて戦略を定期的に見直していますか。	• サイバー・セキュリティがガバナンスや「建物」の基本構造に組み込まれていれば、それは財務委員会や戦略委員会などにとって重要性を持っているはずです。 • 明確かつ実体のある取締役会の委員会、指針文書、標準、主要な監査統制点があることは、いずれもサイバー・セキュリティが組織に組み込まれ、真剣に受け止められていることを示唆しています。 • これが取締役会や上級管理職にとって重要でなければ、スタッフにとっても重要なものとはなりません。したがって、この質問に対して明確な回答を得ることは重要です。
3. サイバー・セキュリティがビジネスの中核的な戦略上および業務上の重点事項であることを実証するものとして、ベンダーはどのようなガバナンス構造を整備していますか。ベンダーにはサイバー・セキュリティに関する専門の取締役会委員会がありますか。 またそれはどのように運営されていますか。	• 上級役員が主導する専門委員会があれば、サイバー・セキュリティが単に技術スタッフに委任された戦術的活動ではなく、会社の優先事項であるということになります。 • 実質的な変革に影響を与え得る主要な取締役会メンバーが委員会に含まれていれば、それがトップ・レベルのコミットメントであるということになります。 • そうした委員会が、サイバー・セキュリティに関する戦略やアプローチの全体的な方向性を定める意思決定機関であれば、取締役会が積極的に関与しているということになります。 • 取締役会メンバーが報告を受けていて、事態が悪化したときにはレビューを行うとともに、危機管理に関与していれば、彼らが業務運営の現場に近い位置にいるということになります。 • 上級管理職が、戦略的な目標や優先事項、利用可能なリソース、総合的なリスク許容度に関して自分たちの期待事項を明確にし、成果の実現における責任の所在を特定していれば、確実に全員がサイバー・セキュリティの重要性を理解していることになります。
4. ベンダーは自らのビジネスにおけるサイバー・セキュリティへの取り組みをどのように保証していますか。取締役会メンバーはビジネスの現状をどのようにして把握し、それに対する説明責任をどのようにして負っていますか。	• トップ・レベルの取締役会委員会がどのようにして戦略の遂行を監督しているかがはっきり示されなければなりません。 • ベンダーは、戦略からビジネスの最前線（お客様の一段階手前）との間に統合された双方向のつながりを持っていなければなりません。 • ベンダーは、取締役会メンバーや上級役員がサイバー・セキュリティに関する対策の実施に対して明確な個人的責任を負っているという証拠を提示することができますか。それとも、彼らは単に委員会に参加しているというだけですか。

要件	さらなる考慮事項
5. ベンダーは、ビジネスのあらゆる部分においてセキュリティの影響を確実に考慮するために、どのようなアプローチを取っていますか。またそれはどのようにして、一貫性のある繰り返し可能な形で実践されていますか。	• サイバー・セキュリティは全員の課題であり、誰もがソリューションの一部でなければなりません。すべきこと、起きてはならないことの判断に対してこのような「全員参加型」アプローチを取っていることを示せれば、セキュリティが確実に企業の DNA の一部であることになります。 • サイバー・セキュリティが「本社」のごく一部の個人に集中すればするほど、ますます「その人たち」だけの問題にしかならなくなります。エンド・ツー・エンドというのは、エンド・ツー・エンドのリソースが関与しなければならないということなのです。 • 社内の他の部署は、どのようにしてこの企業の戦略的方向性に従い、情報を自分たちのリスク管理や業務プロセスに活用していますか。
6. サイバー・セキュリティに関する活動のためのリソース調達に対して、ベンダーはどのようなアプローチを取っていますか。すべてが本社の専門チームを通じて行われていますか。それともリージョナルのセキュリティ・リソースを含め社内の各部署が関与していますか。	• サイバー・セキュリティは誰の問題ですか。それが自分の問題ではなく、自分の能力ではセキュリティに対して最善のアプローチを取ることができないのであれば、誰もその課題には取り組みません。組織設計とセキュリティの組み込み方によって、それが本当に全員参加型の戦略なのか、それとも数人のスタッフによって取り組まれている単なる追加業務なのかがわかります。 • ベンダーは、主要な職務部門のすべてに対して、リスク管理やサイバー・セキュリティがプロセスやリソースを含めた自分たちの活動にどのように組み込まれているのかを実証できなければなりません。 • ベンダーは、社内のプロセスの中で、各地のセキュリティ要件に対する監視と取り組みをどのように行っているのかも実証できなければなりません。
7. どの企業でもセキュリティに関連する事故が発生しますが、ベンダーはそうした経験から何を学んでいますか。学んだことが今後の行動に反映されるように、上級役員はそうした経験をどのようにレビューしていますか。	• 「理解しようとしない」取締役会は、能力の低い取締役会です。よく言われるように、組織のトップにいる人間たちだけが、行動やアプローチの大規模な変革を促すことができるのです。トップの人々がセキュリティに関する欠陥や事故に目を向けなければ、彼らにはお客様が直面している状況を理解することや、自分たちのビジネスの中で自らが直接変えなければならないのは何かを認識することはできません。 • ベンダーは、どのような事故が発生しているか、そうした経験からどのような教訓を得ているか、事故後に物事がどのように改善されているかということを、取締役会レベルの委員会に定期的に報告していることを実証できなければなりません。
8. ベンダーの社内 IT システムは、これまでにサイバー攻撃の被害に遭ったことがありますか。遭ったことがある場合には、その経験から何を学び、自社の製品やサービスの改善に生かしていますか。	• 自らのセキュリティ上の課題から学ぶことができれば、自社のサプライヤーが直面し得る課題と、リスクの観点からのそうした課題を軽減する方法を、より深く理解できるようになります。 • ベンダーは、サイバー・セキュリティに関して「自らに降りかかった災いにどう対処するか」ということを実証できなければなりません。

4.2 標準とプロセス

均一な品質の製品を作り続けるには、一貫した品質管理プロセスや標準、さらに従業員やサプライヤーに対する標準化されたアプローチが必要です。サイバー・セキュリティも同様で、プロセスの中身や標準への準拠に規範性がなければ、最終製品の品質、安全性、セキュリティの水準を均一に維持することができません。

要件	さらなる考慮事項
9. ベンダーは、広義のサイバー・セキュリティに関して何らかの国際標準を採用しサポートしていますか。どのような標準に準拠し、どの標準団体で上位の役職を担ったり、積極的に参加したりしていますか。	• 可能な限り国際標準を採用し、ベスト・プラクティスをビジネス・プロセスに積極的に統合するという企業風土があれば、サイバー・セキュリティに対する最近の考え方と調和する可能性が高いといえます。 • サイバー・セキュリティ標準の策定と採用を推進している標準化コミュニティに参加しているベンダーは、自らもベスト・プラクティスや標準の採用にオープンであるということになります。 • ベンダーは、貴社に必要な技術標準をサポートし、受け入れる姿勢を示していますか。 • ソフトウェアの独立検証の信頼性を高めるため、ベンダーが業界における検証のベスト・プラクティス（コモンクライテリアなど）を採用しているか、自社のサイバー・セキュリティ検証能力とその質の向上に向けて標準化に対するどんな取り組みをしているかについても確認するといいでしょう。
10. ベンダーは、従うべきベスト・プラクティスや標準（あるいは法律）を、どのようにして見極めていますか。どのようなプロセスを経て、法律と標準の間の不一致を見極めて解消していますか。また、どのようにしてそのプロセスを常にアップデートしていますか。	• 標準やベスト・プラクティスに関して問題なのは、「どうあるべきか」が見る人次第で変わるということです。アップデートのメカニズムがあるということは、最新の要件に対応しているということを示しています。物事の見方、標準、アイデアを最大限に幅広く取り入れるためには、他の企業がどのようにして課題に取り組んでいるのかを継続的に評価して、新たなより良い考え方や要件を業務運営に組み込まなければなりません。 • ベンダーは、世界のベスト･プラクティス、標準、規約などを精査し、企業指針、手順、ベースラインに落とし込むための包括的なアプローチを持っていなければなりません。
11. さまざまな技術標準に準拠するための努力として、ベンダーはどのようなチームや機能によって、幅広い管理標準や、暗号方式を含む技術標準に対応していますか。	• この要件リストを拡張して、ISO 27000 シリーズなどの管理／プロセス標準と、X.805、PCI（Payment Card Industry：ペイメント・カード・インダストリー）、OWASP（Open Web Application Security Project：オープン･ウェブ･アプリケーション・セキュリティ・プロジェクト）といった貴社業界向けの技術標準を特定する必要があります。 • ベンダーが既存の標準に対応し、標準の改訂や新たな標準の制定に合わせて技術を変更する準備ができていることも確認する必要があります。 • 暗号方式や暗号化は特殊な分野であり、現地の法律によって規制される場合もあります。ベンダーが暗号方式や暗号専門のリソースを持ち、技術要件だけでなく法律も理解していることを確認する必要があります。

4.3 法律と規制

法律は複雑で多岐にわたり、絶えず改正が行われています。その国に法律があるからといって、必ずしもそれが施行されているとは限りません。また仮に施行されているとしても、その履行方法はさまざまで、同じ法令に対して複数の解釈があり得ます。法律、条例、標準、国際統制によって、サプライヤーや企業にとってより複雑でリスクの高い環境が生じます。

要件	さらなる考慮事項
12. ベンダーは、自らが事業を展開している国のサイバー・セキュリティやプライバシーに関する法律や規制をどのようにして評価し、理解しようとしていますか。そうした情報が、製品やサービスの設計、開発、運用にどのように利用されていますか。	• グローバル企業にとって、事業を展開する国によって法律に食い違いがあることは明らかに困難な課題です。加えて、そうした法律や規約に対する解釈が異なっている場合があることも問題です。したがってベンダーは、法律や規約について絶えず最新情報を入手して評価するためのメカニズムを整備し、自分たちが最新の要件を満たす製品を提供していることをお客様にわかってもらうようにすることが重要です。物事の見方、標準、アイデアを最大限に幅広く考慮するためには、他の企業がどのようにして課題に取り組んでいるのかを継続的に評価して、新たな考え方や要件を自らの業務運営に組み込まなければなりません。 • ベンダーは、世界のベスト・プラクティス、標準、規約などを精査し、それを企業の指針、手順、ベースラインなどの継続的改善に落とし込むための包括的なアプローチを持っていなければなりません。 • 多様で変わりやすく、しかしそれでもなくてはならないという法律の性質を考えると、ベンダーはその製品開発やサービスにおいて、あいまいな法律や相反する法律にどのようにして一貫性のある再現可能な方法で対処するかということを実証できなければなりません。 • 法律は、技術標準や技術要件と同様に重要なものです。ベンダーは、とりわけ個人のプライバシーやデータ保護の分野において、国や地域の法的要件をどのように満たすかということを示せなければなりません。 • 日々のビジネス活動はプロセスに従って行われます。したがって、製品やサービスの設計においてコンプライアンス要件が考慮されていることが実証されれば、あらゆる要件に対する総合的なアプローチが取られていることがわかります。
13. ベンダーは、どのようにして自社のプロセスを現地の法律や要件と確実に整合させていますか。現地の法律が自社の指針、標準、プロセスと相反するものである場合、ベンダーはそれにどのように対処しますか。ベンダーは、政府機関との関係に関する公式声明を出していますか。	• 法律は法律であり、ベンダーは自社の機器やサービスが法律に沿ったものであることを示せなければなりません。 • 自国外で事業を展開している企業はいずれも、各国オフィスの要望や見解が確実に本社に届くようにすることを課題としています。ベンダーは、こうした海外オフィスからの要望や見解がどのようにして本社の考え方や製品開発に反映されているかを示せなければなりません。 • ベンダーは、優先する現地の法律と相反する法律や要件にどのように対処するかを示せなければなりません。 • ベンダーは、情報やデータを他国の政府に提供する何らかの義務を負っているかどうかを明示できなければなりません。 • ベンダーは、国家安全保障、「バックドア」の設置、暗号やセキュリティ保護の弱体化などに関していずれかの政府機関と関係があるかどうかを開示しなければなりません。 • ベンダーは、データがどこに保管され、どこの法域がそのデータの管轄権を有するのかを明示できなければなりません。
14. ベンダーは、プロセスや製品が配備されている国の輸出規制法と事業運営法（暗号方式を含む）に従ったものであることを、どのようにして保証していますか。	• ベンダーは、販売からサービス、契約、製品設計まで、全プロセスを網羅する統合されたガバナンス、指針、手順があること、それらが貿易コンプライアンス、ライセンス管理、輸出規制などあらゆる領域における具体的な法的要件に準拠していることを実証できなければなりません。 • また、主要な要件が満たされているかどうかを確認するための適切な管理項目があることも実証できなければなりません。 • それができない場合には、購入者が法律に違反する機器やサービスを交換しなければならなくなるリスクを負うことになります。

要件	さらなる考慮事項
15. ベンダーは、IPR（Intellectual Property Rights：知的財産権）に対してどのような企業指針を定めていますか。	• 企業は、ライセンス付与、IPR、異文化間の相違などへの対応について詳述した指針、手順、アプローチを制定できなければなりません。倫理的課題や法的課題はさまざまな国で発生しますが、対応は一貫したものでなければならず、またそれが企業の一連のビジネス手法の中に組み込まれている必要があります。ベンダーに社内行動規範や業務行動指針があることを確認すべきです。
16. ベンダーは、どのようにして自社の営業チームが、輸出規制や貿易制裁も含めた現地の法律や規制に準拠した製品やサービスのみを販売していることを保証していますか。	• 営業チームの役割は製品やサービスを販売することです。それが彼らのモチベーションであり、またビジネスの成功には欠かせないものでもあります。彼らは、規則や規制が販売の妨げになると考えていることもあります。また、購入者が調達の管理に十分なリソースを割けない場合もあります。したがってベンダーは、自社のプロセスがどのように購入者を保護するのかということを実証できなければなりません。 • ベンダーは、販売、法務、デリバリーやサポートを統括する、購入者の社内外の要件に合致した統合プロセスを明示できなければなりません。
17. ベンダーは、どのようにして契約書のレビューを行い、サイバー・セキュリティに関する能力について正確な情報が記載されていることを保証していますか。	• プロジェクトや契約書は非常に複雑で長期間にわたることが多く、多数の企業のさまざまな部署からの協力を得て成立します。ベンダーは、法律や規制も含めて、合意事項や契約事項が購入者の目的を満たすものであることを実証できなければなりません。
18. ハイテク分野の大企業はいずれも他のベンダーのテクノロジーを利用しています。これを踏まえ、ベンダーはライセンス付与や制御のメカニズムを整備していますか。	• ベンダーが利用しているサードパーティのコンポーネントが、適切にライセンスを取得していることを確認する必要があります。そうすることで、ハードウェアやソフトウェアの交換を余儀なくされ、業務中断によりコストがかさむという事態を回避できます。

4.4 人　材

多くの企業は人材が最も重要な資産であるとしており、これは確かに事実です。しかし、セキュリティの観点からは、人材は最大の弱点ともなり得ます。多くの場合、成功も失敗も従業員の雇用、教育、動機づけ、業績管理をどのように行うかにかかっています。これはサイバー・セキュリティに限ったことではなく、企業戦略全体の成否にも同じことが言えます。

要件	さらなる考慮事項
19. ベンダーは、全従業員を対象にしたサイバー・セキュリティへの意識向上教育に経営陣を参加させていますか。参加させている場合、それはどのようにして行われていますか。ベンダーの上級役員や取締役会は、法令のコンプライアンスに関する研修を継続的に受けていますか。	• 意識向上教育は、中間管理職も含めた経営陣にとって重要な問題とみなされていなければなりません。そうでなければ、一般の従業員から軽視されてしまいます。したがって、経営陣は全従業員を対象にした意識向上のための研修を重要なものとして位置づけるとともに、自らそれに参加することで言動を一致させるべきです。 • ベンダーが、「私たちは全員が仕事に熱意を注いでいる」ということ、「それは私たち１人ひとりの責任である」ということを実証できるのであれば、うまくいく確率は高いでしょう。 • 企業の意思決定者と日常業務の監督者が法令コンプライアンスを理解していれば、安定的かつ継続的な業務運営が可能になります。これらの人々は、サイバー・セキュリティに関する法律の知識を持っていなければなりません。

要件	さらなる考慮事項
20. すべての役職が等しく内部脅威になるリスクを持つわけではありません。ベンダーは、サイバー・セキュリティにとって「重要」または「最重要」の役職を特定していますか。	• お客様にサービスを提供する「最重要」の役職には必ず信頼性の高い人材を置き、不可欠な防御手段を提供しなければなりません。 • 「最重要」の役職を特定するためのメカニズムが確立されており、それらの役職の潜在的リスクに焦点を当てて効果的に管理できていれば、そのベンダーは成熟していると言えます。 • 例えば、自社の中核的な ICT に直接アクセスすることができ、製品ソフトウェアを直接変更できる役職は、製品やサービスにより深刻な脅威をもたらす恐れがあります。
21. ベンダーは、「重要」または「最重要」の役職に配属される従業員の採用と審査にあたり、どのようなアプローチを取っていますか。	• この質問からは、人材の資質と完全性に対する一貫したアプローチがあるかどうかがわかります。こうしたアプローチは、内部脅威のリスクをどのように認識し、それをどのように軽減しているかを示しています。 • これを実証できるベンダーは、サイバー・セキュリティに対して総合的なアプローチを取っているということです。
22. ベンダーはどのようなプロセスやメカニズムによって、従業員の職責、指針、手順などの要件と一致した形で、サイバー・セキュリティに関する定期的な意識向上研修や特定の項目に関する研修を行っていますか。ベンダーは、従業員によるそうした研修の受講状況をどのようにして把握していますか。	• ベンダーはどのようにしてサイバー・セキュリティを全従業員に浸透した企業文化の一部としていますか。そのためにどのような基本的なシステムや手順を整備していますか。 • サイバー・セキュリティは長期的な要件であり、そのため各人が頻繁に新しい知識を取り入れていかなければなりません。ベンダーの知識が常に最新の状態に保たれていなければ、焦点がずれたり準備が不足したりすることになるでしょう。 • ベンダーが定期的な意識向上研修を行っていて、グローバルとローカルのさまざまな意識向上ツールを利用しているかどうか、また職務領域ごとに追加研修（特定の項目に関するより詳細な研修）を行っているかどうかを見極めるといいでしょう。従業員やパートナーが、関連する指針、手順、合意事項と一致した形で、情報やサイバー・セキュリティに関連する責務を果たすための十分な研修を受けていることは確認しておきたいものです。
23. ベンダーには、「重要」または「最重要」の役職に就く従業員の能力と理解の向上に重点を置いた指針がありますか。	• これはつまり、特定の役職を「重要」または「最重要」としているならば、通常とは異なる厳格な要件が課せられているはずだということです。ベンダーは、お客様に対するリスクというのは単に知識として知っていればいいわけではなく、経験や、完全性などの価値観も必要だと理解していることを示せなければなりません。
24. 多くの国には贈収賄防止や汚職防止に関連する法律がありますが、ベンダーは自らの従業員がそれらの法律を遵守するためにどのような取り組みを行っていますか。	• ベンダーは、贈収賄や汚職の防止対策に関する各国ごとに異なる法律や国際的に受け入れられているベスト・プラクティスを、どのようにして従業員に周知しているのかを実証できなければなりません。 • ベンダーは、自社の価値観と善悪の判断基準をどのようにして一貫した形で従業員に周知させ、従業員の意識に植え付けていますか。
25. ベンダーには、従業員が指針、法律、または規制に反しているかもしれないと感じる事象に遭遇した場合、それを（適切な方法で）経営陣に連絡できるメカニズムがありますか。	• 企業の従業員は往々にして、経営陣の目には触れないようなことを知っています。連絡メカニズムを確立することにより、企業は早期に問題を発見してそれを改善できるようになります。自己学習型のクローズド・ループ式改善システムがあれば、自社のプロセスに適合しない事柄に会社としてどのように取り組んでいるのかがわかります。従業員がおかしいと感じたことを報告できるようにするには、多くの場合そうしたメカニズムが必要です。
26. ベンダーは、従業員退職時にどのような施策を実施していて、そのプロセスで得た知識をどのように指針、手順、文化の改善に利用していますか。	• 従業員が退職する理由はさまざまですが、中には自分が目にしたことを不快に感じて会社を去る人もいます。こうした従業員からのフィードバックにより、セキュリティ上の問題点が発覚する場合があります。ベンダーは、問題を解決してビジネスを改善するための方法として、退職していく従業員からのフィードバックも含めたあらゆる形の意見や情報を、会社の運営の仕方とその指針や手順に反映させているということを実証できなければなりません。

要件	さらなる考慮事項
27. ベンダーには、サイバー・セキュリティに関する賞罰を定めた正式なガイドがありますか。	• ベンダーは、お客様、会社、従業員にとって正しいセキュリティ文化を生み出すために報奨と罰則のバランスをどのように取っているかを示せなければなりません。 • 従業員がサイバー・セキュリティに関する会社の指針に故意に違反した場合には、どのような指針やプロセスが採用されて、違反者に対してどのような懲戒処分が下される可能性があるかということを、明確にしておく必要があります。
28. 従業員に対して懲戒処分が下された場合、ベンダーは管理者や監督者の職務怠慢の可能性に対する責任をどのように追及しますか。つまり、管理者や監督者も問題視しますか。	• ベンダーは、管理者が自分のチームの業績と行動に対して責任を負っていて、それについて他の人のせいにすることはできないということをはっきりと示せなくてはなりません。従業員個人、管理者、チームに対する説明責任と賞罰のバランスをどのように確保しているかを実証できなければなりません。

4.5 研究開発

企業は限られた資本を投入してハイテク製品を購入するにあたり、常に高品質で安全な製品を納品できる厳密な R&D（Research and Development：研究開発）プロセスを持ったベンダーでなければ取引したいとは思わないでしょう。さらに、「新製品に投資するか」「全製品の安全性確保に投資するか」のどちらか一方を選ぶベンダーとも関わりたくはないでしょう。品質を製品に後付けできないように、サイバー・セキュリティも後付けすることはできません。企業は次世代製品に投資すると同時に、サイバー・セキュリティを適切な形で製品の設計・開発・展開に組み込むよう R&D を強化するという長期的な姿勢を示すことが必要となります。

要件	さらなる考慮事項
29. ベンダーには、サイバー・セキュリティの要件が組み込まれた一連の正式な研究開発プロセスがありますか。またそれは、何らかの業界標準やベスト・プラクティスに基づいていますか。	• ベンダーが研究開発に対する一連の成熟したプロセスやアプローチを持っていることを実証できない場合、そのベンダーには品質とサイバー・セキュリティを組み込むための礎となる確固たる基盤がありません。成り行き任せのプロセスは、成り行き任せの品質、成り行き任せのセキュリティ性能、そしてリスクの増大につながります。 • セキュリティに対する完全なモデルや単一のグローバル標準はないため、ベンダーはさまざまなソースから得た知識とベスト・プラクティスをどのように活用しているかを実証する必要があります。
30. ベンダーの研究開発プロセスは、動的な脅威環境を含めたサイバー・セキュリティの要件をどのように満たし、その有効性をどのように評価しますか。ベンダーは、何が必須で何が単に優れた慣行であるのかを見極めるために、どのようなメカニズムを利用していますか。	• 多くの人々はこれからもサイバー・セキュリティを品質の一部とみなし続けると思われますが、これにはさまざまな要素が含まれています。とりわけ、脅威は動的なものであり、攻撃のための侵入点は実に多様です。ベンダーは、セキュリティ要件を研究開発に組み込み、新たな問題や知識を見つけ出し、セキュリティ性能の有効性をテストするという、クローズド・ループ式アプローチを実証できなければなりません。有効性がない場合には、まずそれに変更を加え、最初に戻って新たな知識や修正された知識、学習した事項を組み込んで、サイバー・セキュリティを強化しなければなりません。

要件	さらなる考慮事項
31. 世界各地のお客様にはさまざまな要件があり、それらは時として相反する場合もあります。ベンダーには、お客様の要件を取引関係が終了するまで考慮し、この先に起こり得ることやなすべきことを評価する、一連の統合されたプロセスがありますか。	• 国によって異なる法律や規制、社会文化、ユーザーの嗜好に応じて、お客様ごとにさまざまな要件が生じます。固定された柔軟性のないプロセスでは、特定のお客様や地域に固有の要件を満たすことはできません。適切な管理が欠如していると、お客様が得たものが期待はずれであったり、さらには希望している機能とは正反対のものであったりという結果を招く場合があります。ベンダーは、それぞれに異なる要件や相反する要件に対して、効果的な管理能力を示すことができなければなりません。
32. ベンダーには、製品をライフサイクルが終了するまでサイバー・セキュリティの観点から管理し続けるライフサイクル戦略がありますか。そこからどのようなことがわかり、またベンダーはそれをどのように利用していますか。	• 自分が購入しようとしている製品に、購入経費を回収できるだけの適切な耐用年数(例えば3～5年)が備わっていることを確認する必要があります。ベンダーは、製品単体または関連製品一式のライフサイクルの管理にどのように取り組むのかを詳しく説明できなければなりません。つまり、販売する製品が短期間で陳腐化したり、アップグレードできなくなったりはしないということを保証できなければなりません。 • セキュリティ要件が機能や性能、信頼性といった他の要件と相反する場合、ベンダーは優先すべき要件をどのように判断しますか。
33. ベンダーの主要な製品開発プロセスはどのように機能していますか。ベンダーは開発の進捗状況をどのようにレビューし、技術と品質の観点からどのように継続的改善を行っていますか。また、そのプロセスにどのようなレビュー、チェックポイント、決行／中止の決定点が組み込まれていますか。	• 大半の技術は複雑であるため、ベンダーが自らのプロセスに、複数回にわたる技術的レビュー、ビジネス・レビュー、セキュリティ・レビュー、品質レビュー、チェックポイントをどのように組み込んでいるのかがわかれば、ベンダーが目標と追求すべき成果を決して見失っていないという安心感を得ることができます。
34. 現代のソフトウェアは非常に複雑で、通常、数百万行に及ぶソース・コードと、さまざまなサプライヤーからの何千ものコンポーネントが組み込まれています。ベンダーは、適切なコンポーネントを適切な用途で使用するために、どのような手順や技術を利用していますか。	• 開発プロセスを明確に定義できたとしても、そのプロセスをサポートするための効果的な IT 管理プラットフォームがなければ、社内規制やお客様の要件を満たすことは難しいでしょう。最終的なコンピューター・システムを形成するさまざまな要素が「コンフィギュレーション管理」に組み込まれていなかったり、適切に制御されていなかったりすると、システムが一貫して機能しない可能性があり、また何がどこで使用されているのかをトレースして特定することができません。
35. コンフィギュレーション管理はシステム・エンジニアリング・プロセスであり、ライフサイクル全体を通して、製品の性能、機能的属性、物理的属性の一貫性を維持するためのサポート技術が必要とされます。複雑な技術環境では、このメカニズムが、一貫した質の高いセキュアなコードを作成する基盤になります。ベンダーはこれに対してどのようなアプローチを取っていますか。	• ベンダーは、技術要素に故意に手が加えられたり、製品の開発やコンパイルに間違った要素が組み込まれたりするのを防ぐ、体系的な「コンフィギュレーション管理」や制御システムがあることを実証できる必要があります。 • こうしたシステムには、バージョンと変更の管理、サードパーティのツールとコンポーネントの管理が含まれていなければなりません。

要件	さらなる考慮事項
36. 脅威や潜在的ダメージを抑えるためには職務の分離が重要ですが、ベンダーは研究開発の中で、特にソフトウェア・エンジニアに対して、どのようにしてこれを実行していますか。	• どうすれば内部脅威が軽減されるかを理解することが大切です。職務の分離は内部脅威を回避するための重要な手段の 1 つです。ベンダーは、研究開発に関わる職務を特定し、それぞれの職務が研究開発プロセスのどの部分に関与するのかを明確にできなければなりません。セキュリティの観点から見ると、個人がアクセスできるフェーズ、作業、製品、ソース・コードを制限できれば、リスクも限定できます。
37. 多くのテクノロジー企業は自社のコンピューター・コードにサードパーティ・ソフトウェアやオープンソース・ソフトウェアを組み込みますが、ベンダーは、自社の各製品内に何が含まれているのかをどのようにしてトレースし管理していますか。	• ベンダーのコードやコンピューター・テクノロジーが高い水準で構築されていても、それに使用されている他のベンダーのテクノロジーの中に弱点が存在しているかもしれません。どこに問題があり、どのベンダーのソフトウェアやハードウェアが関与しているのかを知ることが、リスクを評価して修正措置を講じる上で重要なステップになります。
38. オープンソースやサードパーティのソフトウェアは、たいてい複数のウェブサイトで見つかります。ベンダーは、自分たちがダウンロードするソフトウェアが合法で、そこにはマルウェアやバックドアが仕込まれていないことをどのようにして確認していますか。	• どのようなソフトウェア・コンポーネントが使用されていて、自分たちがそれらをどこから調達しているのかということを、ベンダーが厳格に管理していない場合、それは十分な品質管理がなされていないことを示しています。逆に、信頼できるサイトからしかソース・コードを取得しないようにするきわめて厳格なプロセスがベンダーにある場合、それはリスク軽減要因となり得ます。 • 一部の危険なサイトでは、オープンソース・コードに手を加えてマルウェアを仕込んでいる場合もあるため、ベンダーは警戒しなければなりません。
39. ベンダーは、サードパーティのソフトウェアを使用する場合、その使用を決定する前およびそれを採用した後に、どのようなプロセスを経て既知の脆弱性がすべて解決されていることを保証していますか。	• 購入者も販売者もともに ABC（Assume nothing, Believe no one, and Check everything：先入観を持たず、誰も盲信せず、すべてを確認する）モデルに従うことが重要です。ベンダーは製品を出荷する前に、その製品に組み込んだサードパーティ・ソフトウェアの既知の脆弱性がすべて修正されていることを立証できなければなりません。製品が発売された後に新たな脆弱性が見つかる場合もあるため、これは継続的なプロセスにする必要があります。 • ベンダーがサードパーティのコンポーネントを製品に使用している場合、そのサードパーティ・ソフトウェアが製品のライフサイクル終了まできちんと管理されるかどうかをベンダーに確認したほうがいいでしょう。
40. ベンダーは、サードパーティのソフトウェアやオープンソース・コンポーネント、さらにソフトウェアの共通ルーチンにおいて、すべての箇所でバグが修正されていることを、どのようにして保証していますか。	• サードパーティ・コンポーネントは、複数のベンダーの製品や、同一製品内でも複数の箇所で使用される場合が多くあります。したがって、サードパーティの脆弱性を修正するには、ベンダーがそのコンポーネントを使用しているすべての製品を把握している必要があります。さもなければ、脆弱性が修正されないままの製品が出てくるリスクが生じます。
41. ベンダーは、自社製品において複数の開発言語やツールを使用していますか。その場合、ベンダーはそれらのツールをどのように記録し、それが最新かつサポートされているバージョンかどうかをどのように確認していますか。	• ベンダーが多数のサードパーティのさまざまなツール、ソフトウェア、コードを使用している場合、製造元企業の合併、倒産、戦略の変更の影響を受ける可能性があります。そのため、ベンダーに、サードパーティの製品やコンポーネントを品質、アーキテクチャ、製品開発ロードマップに基づいてレビュー、承認、拒否する正式なプロセスがあることを確認すべきです。 • ベンダーは、自社の製品にはサポートされていて安全なサードパーティのツールやコンポーネントのみが組み込まれているということを保証する戦略やメカニズムを示す必要があります。

要件	さらなる考慮事項
42. ベンダーは、エンド・ツー・エンドの研究開発プロセスと、使用しているオープンソース・ソフトウェアやサードパーティ・ソフトウェアそれぞれを、どのように記録・トレースできるようにしていますか。	• 物事が間違った方向に進むこともあれば、人々が悪事を働くこともあります。もし何かが起きてシステムがダウンしたり、何らかの危険にさらされたりした場合、ベンダーには問題を見つけ出すまでにどれだけの時間的猶予を与えますか。1 日ですか、1 週間ですか、1 か月ですか。複雑なテクノロジーには、数千に及ぶコンポーネントと、何百万行ものソース・コードが含まれています。ベンダーは、すべての会社に販売したすべての製品において使用されているすべてのコンポーネントをトレースできなければなりません。購入者も、これまでに購入したすべての製品をトレースできなければなりません。またベンダーは、プロセスに関与しているすべての人々と、彼らがいつ何をしたかということ、さらにはその作業に対するすべての権限までトレースできなければなりません。
43. 複雑な製品のソース・コードは多くの場合、数百万行に及びます。ベンダーには、研究開発の一部としてコーディング作業を自動的にテストする自動化されたコード・スキャン環境がありますか。	• 優れたエンジニアリングでは、できるだけ多くの作業を自動化することで、品質の保証と一貫性の促進を目指そうとします。ベンダーは、製品のさまざまな問題を動的にスキャンするための自動化されたツールや手法を複数持っている必要があります。そうしたスキャンの結果がベンダーの品質管理システムに自動的にフィードバックされるようになっていればなお理想的です。 • 自動化だけでは、あらゆる問題を検出してすべてを解決することはできません。そのため、複合的なアプローチを取って、技術による検証のみに依存しすぎないようにする必要があります。
44. ベンダーは、製品を市場にリリースできるかどうかをどのようなメカニズムで判断し、それをどのようなプロセスで承認していますか。	• 承認プロセスの厳格さについて確認したほうがいいでしょう。社内外の ICT チームから「95% 完成した」という発言を聞くことが多くあるかもしれません。しかしベンダーは、製品があらゆる点で 100% 完成していることを証明できなければなりません。これには、プロジェクトに関与していないチームのメンバーによるレビューが必要です。 • ベンダーは技術保証、品質保証、セキュリティ・レビューを複数回実施しているという証拠を示せなくてはなりません。また、最終的な承認については、ソフトウェア・エンジニアにその決定を委ねるべきではありません。自分の宿題を自分で採点してはいけないのです。
45. 欠陥は製品開発サイクルと製品のライフサイクルのどの時点でも生じ得ます。ベンダーは、どのようにしてすべての欠陥をトレースし、該当するコンポーネントが使用されている可能性のあるすべての製品においてその欠陥を修正しますか。	• 同じ問題が何度も繰り返し発生したり、別々の製品で発生したりという経験は避けたいものです。したがって、ベンダーが欠陥や問題をどのようにトレースし、それを研究開発や研修などさまざまな分野にどのように反映させているかということを知る必要があります。
46. ベンダーは、サイバー・セキュリティに関する自社のコンピテンシーの成長を、どのようにして最大化していますか。中核的研究拠点やセキュリティ・スキル・センターを運営していますか。それはどのように機能していますか。	• 誰もがあらゆる分野のエキスパートになれるわけではありません。大規模で複雑な技術エンジニアリングにおいてもこれは同じです。したがって、ベンダーは自社のセキュリティ能力の幅と深さを評価して、適切なチームがこの重要なスキルと専門知識にアクセスできるようにする必要があり、購入者はそれがどのようにして行われるのかを知る必要があります。
47. 脅威というのは絶えず形を変えて発生し続けるものですが、ベンダーはどのようにしてそれらを監視し、設計、開発、展開の各フェーズでどのようにそれらを考慮に入れていますか。	• 常にバックミラーばかり見ながら車を運転していたら、壁に突っ込んでしまいます。ベンダーは、前方に目を向けて次の問題を予測し、製品の設計や開発においてそれらに対処していることを示す必要があります。 • ベンダーは、自分たちが脅威や攻撃のあらゆる発生源を考慮していることを実証できなければならず、またそれが設計やその他の要件にどのように反映されているのかも示せなければなりません。

要件	さらなる考慮事項
48. ベンダーのプロセスは関連する技術によってどのようにサポートされていますか。例えば、ベンダーはテストにおいて脅威データベースをどのように利用していますか。あるいは、ベンダーはテスト・ケースのライブラリーを構築していますか。	• ベンダーは、プロセスや標準について聞こえのいい話をするだけでなく、しっかりとサポートされ統合された技術によってそれらを支えることで、効率と効果を保証しなければなりません。 • ベンダーは、プロセスや業務部門ごとに、業務とビジネス目標をサポートするための一連の統合された技術プラットフォームを整備していなければなりません。
49. ベンダーは、リリース管理に対してどのようなアプローチを取っていますか。すべての国のすべてのお客様用に単一コード・ベースを保有しているベンダーもあれば、1つのコード・ベースと特定の地域・国・お客様用のブランチを保有しているベンダーもあり、どちらの方法にも長所と短所があります。そのベンダーはどちらのアプローチを取っていますか。	• 全世界で1つの製品を展開するか、国やお客様ごとに1つの製品を展開するかについて、正しいモデルというものはありません。全世界を対象に1つの製品しか展開しない場合には、柔軟性が下がり、ベンダーは要件に対応したがらなくなるかもしれません。一方、似たような機能を持つ数百種類もの異なる製品を展開する場合は、サプライヤーのコストが上昇し、効率性が低下することになります。重要なのは、ベンダーがどのようにして適切なバランスを取り、その選択に伴う課題をどのように管理しているかを理解することです。

4.6 検証：先入観を持たず、誰も盲信せず、すべてを確認する

高品質で安全な製品を提供するにはしっかりとしたR&Dプロセスが不可欠ですが、R&D部門は適切な試験や検証なしで新製品をすばやく市場に投入しなければいけないというプレッシャーにさらされる場合もあります。独立した検証において「多くの目、多くの手」という方針で複数の階層を設定すれば、安全性に欠ける製品が出回るリスクを低減できます。全過程で抑制と均衡を保てば、「近道をしない」アプローチでお客様の投資とサービスを守ることができます。

要件	さらなる考慮事項
50. ベンダーには、製品が市場にリリースされる前に、研究開発プロセスのほかにも、その製品について独立した検証（製品の開発者以外の第三者によるテスト／検証）を行うサイバー・セキュリティ・ラボがありますか。	• 研究開発チームには独自の事業目標があります。彼らは、進捗状況、コスト、セキュリティのバランスを取る必要があるのです。研究開発チームから独立したラボなら、研究開発チームの影響を受けることなく、セキュリティ目標の達成に注力することができます。またこのアプローチは、職務の分離によってリスクを低減する方針とも一致します。 • ベンダーは、製品を発売前に適正な状態にすることを重視しているという姿勢を示せなければなりません。
51. ベンダーの研究開発チームやマーケティング・チームがこのラボによるテスト結果を無視することはありますか。	• 品質と完全性の観点から見ると、製品がすべての品質およびセキュリティ要件を満たしていることを、プロジェクトに関与していない人々が確認すべきです。こうした人々は、組織内におけるその他のいかなる部署からも影響を受けてはなりません。彼らには拒否権を与えるべきです。 • 先に論じたガバナンスと関連しますが、ベンダーには社内のラボで見つかったあらゆる問題を上級経営陣に報告する制度がありますか。

要件	さらなる考慮事項
52. ベンダーが運営するいずれかの社内ラボで、侵入テスト、静的および動的コード・スキャンを行って、コードが設計とコーディングにおけるサイバー・セキュリティ要件を確実に満たすものになるようにしていますか。こうしたラボでは、評価報告を利用して、製品チームに改善を強く促していますか。	• このようなラボの目標は、セキュリティに関連するあらゆる問題に焦点を当てることです。したがって、ベンダーにそうしたチームの幅と深さを示してもらえば、ベンダーのセキュリティ・アプローチが盤石であることがわかります。 • しかし、品質を推進するためには、ベンダーはこの検証やテストで見つかった問題を、テスト対象の製品の改善だけでなく、自社の研究開発の基本構造の改善にまでどのように活用しているのかを示せなくてはなりません。
53. ベンダーは製品を、本社の支配が及ばない他の独立したセキュリティ検証に出していますか。出している場合、それはどのような検証で、どう機能していますか。	• テスト･チーム間にある程度の競争があり、さまざまなツール、手法、アプローチを採用していれば、あらゆるセキュリティ・テスト・プロセスの完全性と強固さが向上します。ベンダーのこうしたプロセスへの投資が厳格かつ高額であるほど、長期的なセキュリティと品質の確保に対して戦略的に取り組もうとしていることがわかります。
54. ベンダーはお客様や政府機関に対して、社内または社外のラボで独自のスタッフやセキュリティ・アドバイザーによる製品テストを行うことを認めていますか。	• 自社製品の品質の検証を外部者にまで認めるというベンダーのオープンな姿勢は、自分たちのアプローチに対する自信と信頼を表しています。常に密室で行われているようでは、そのベンダーが品質やセキュリティに対してどれだけ真剣に取り組んでいるか疑問です。
55. お客様や政府機関が、サードパーティが運営する独立したセキュリティ・ラボの使用や、コモンクライテリア（またはそれに類するアプローチ）の採用を希望した場合、ベンダーはそれを承諾あるいは検討してくれますか。	• ベンダーが独立した評価のためのさまざまな方法を受け入れ、場合によっては外部者と合同で行うことさえ認めるのであれば、そのベンダーはセキュリティに対するコミットメントが高いことになります。 • 購入者は、自らのプロジェクトのリスクと契約の規模に基づいて評価方法を選択できるような柔軟性を望むかもしれません。
56. ベンダーが本社や事業グループの下にある場合、本社や事業グループは社内または社外のラボの独立性を制御したり妨げたりしますか。また、レポートや評価報告書をお客様や政府機関に提出する前に、それらを読んで修正を入れる権利を保有していますか。	• 時としてベンダーは、製品の発売の必要に迫られたり、契約を取りたいがために好印象を与えたいと考えたりする場合があります。製品の独立したテストの有効性を主張するのであれば、ベンダーはそのプロセスの結果が外部からのいかなる影響も受けていないこと、あるいは発売やその他の圧力のために手が加えられたという事実がないことを実証する根拠を示せなければなりません。 • 評価プロセスに基づく報告書はいずれも、潜在的な脆弱性が知られてしまうのを防ぐことを目的とする場合を除き、お客様やその他の適切なステークホルダーに送付される前に会社によって修正されることがあってはなりません。
57. ベンダーの本社の研究開発グループは、社外のラボで利用されているツール、プロセス、スクリプトのいずれかにアクセスすることができますか。ベンダーの本社は、ベンダーがテスト結果に影響を及ぼすことができるように、テスト内容を推測し得る可能性はありますか。	• ベンダーの本社がどうすればラボが「良」と評価するのかを知っている場合、ラボのツールが製品を「良」とみなすように本社が製品に細工をすることは可能ですか。機密保持に対する厳格なアプローチを保有していれば、いかなるラボも品質とセキュリティの向上を唯一の目的としていることを示していると言えます。

要件	さらなる考慮事項
58. ベンダーのラボや検証センターにおいて欠陥や潜在的な脆弱性が見つかった場合、研究開発チームが確実にその問題を修正して今後の製品で再発しないようにするために、どのようなプロセスが実施されますか。	• 何らかの異常を報告したにもかかわらず、報告後も何ひとつ改善されていないというのはよくあることです。ベンダーは、あらゆる問題や欠陥にどのようにして体系的に対処しているかということを示せなければなりません。ベンダーは、特定されているすべての問題と、それらの問題を解決するためにどのような措置が取られたかということを明確にできるべきです。同時に、問題が発生した本当の理由への理解を示し、再発防止に向けてプロセス、研修、テンプレートなどを変更するためにどのような措置を講じているのかを明らかにすることも重要です。
59. ベンダーのラボや検証センターには、修正やパッチの適用が行われた後にソフトウェアの再テストを行って、問題が本当に解決されていること、それ以外には何も手を加えられていないことを確認する能力がありますか。	• 品質やセキュリティの保証は 1 度のテストで済むような問題ではありません。テクノロジー、脅威、製品の用途は変化します。ラボやサードパーティには、製品の再テストと、製品の変更やその他の修正が行われた後の変更点の再テストを行う能力がなければなりません。
60. ベンダーは、検証センターから学んだことを、どのようにして自らのビジネス・プロセスに体系的に統合していますか。	• ベンダーの社内外でのテストやお客様によるテストにより、特定の製品上の問題に加えて、システムの問題が見つかる場合があります。ベンダーが総合的な統合アプローチを用いている場合、どのようにしてこうした情報を取り入れて根本的な問題に取り組んでいるのかを具体的に示すことができなければなりません。

4.7 サードパーティ・サプライヤーの管理

多くの大規模なハイテク企業は、ハードウェアおよびソフトウェアのコンポーネントの調達、デリバリーのサポートや製品の設置においてサードパーティを利用しています。サードパーティの技術やプロセスにセキュリティの脆弱性があると、それを統合した製品やサービスの脆弱性も高くなります。エンド・ツー・エンドのサイバー・セキュリティを実現するには、サイバー・セキュリティのベスト・プラクティスをサプライヤーと連携して取り入れていかなければなりません。

要件	さらなる考慮事項
61. ベンダーは、どのようにして自社のサプライヤーのセキュリティ管理を行っていますか。ベンダーは、適切なセキュリティ基準を設定して、それを自社のサプライヤーに伝えていますか。ベンダーは、最新の考え方に後れを取らないようにするために、どれぐらいの頻度で基準を更新していますか。	• ベンダーのサプライヤーのセキュリティ管理は不可欠です。ベンダーは、自社とお客様のそれぞれのサイバー・セキュリティ要件を、サプライヤーに伝えなければなりません。それができていなければ、お客様が受け取るコンポーネントにはベンダーのサプライヤーに由来するセキュリティ上の弱点が含まれている可能性があります。 • ベンダーは、自分たちが準拠している業界のセキュリティ標準や独自に設定したセキュリティ基準を、自社のサプライヤーにどのようにして伝えているかを示せなければなりません。設定された基準は常に最新の状態に保ち、最新の考え方やセキュリティの知識を確実に反映するようにする必要があります。 • ベンダーは、自社のサプライヤーがサイバー・セキュリティに関連する活動に必要なスキルを持った人材を十分に充てていることをどのように評価していますか。ベンダーはサプライヤーに特別なサイバー・セキュリティ・チームを組織するよう要請していますか。 • ベンダーには、自社のサプライヤーにサイバー・セキュリティの要件、基準、知識を不足なく伝えるための特別な役職、組織、プロセスがありますか。

要件	さらなる考慮事項
62. ベンダーのサプライヤーは、自社のサプライヤーに対してどのような調達プロセス要件を考慮していますか。	• あらゆるベンダーのサプライヤーが、すべてのセキュリティ要件を満たせるということはまずありません。セキュリティ面の弱いサプライヤーを利用するリスクを確実に抑えるために、ベンダーのサプライヤーに対するセキュリティ「認証」とレビューが必要です。 • ベンダーが、サプライヤーにサイバー・セキュリティの課題にベンダーとともに取り組むことを義務付けるプログラムの一環として、適格なサプライヤーとしての資格を付与するセキュリティ「認証」を要求すれば、サプライヤーはベンダーから課された基準を満たせるよう自らのセキュリティ能力を向上させるようになるでしょう。 • ベンダーはサプライヤーの選定にあたり強固なセキュリティ重視のプロセスを有している必要があり、そのプロセスにはサプライヤーのパフォーマンスの評価、監視、改善をどのように行うかが含まれていなければなりません。
63. ベンダーは、コア技術のサプライヤーとの間で契約条項やセキュリティ協定を整備し、リスク情報に基づく一連の包括的な要件をサプライヤーが満たすべきものとして提示していますか。	• ベンダーのサプライヤーは、セキュリティに関して自分たちに何が期待されているかを知っていなければなりません。セキュリティ協定は、セキュリティ要件と法的義務をサプライヤーに伝えるための適切な方法です。セキュリティ協定はサプライヤーにセキュリティ管理の強化を義務付けるとともに、サプライヤーが提供するすべての製品のセキュリティに対して契約上の責任を負わせることができます。 • ベンダーは、調達先を問わず製品に使用されるすべてのコンポーネントがセキュリティの手順と要件を伴い、それらに準拠していることを、契約や協定によってどのように保証しているのかを示せなくてはなりません。
64. ベンダーは、サプライヤーがセキュリティに関する条項や協定にどれだけ準拠しているかを評価するために、どのようなプロセスを整備していますか。ベンダーは、説明責任の促進とパフォーマンスの推進のために、スコアカードやその他の評価基準を保持していますか。	• ベンダーのサプライヤーは替わる場合があり、セキュリティの問題はいつでも発生する可能性があります。ベンダーは、サプライヤーとどのように連携してパフォーマンスを評価し、また両者でどのように協力して問題を解決しているかを実証できなければなりません。その方法としては、スコアカード、監査、検査などがあります。
65. ベンダーは、サプライヤーが自社製品に脆弱性を発見した場合、ベンダーに報告するよう義務付けていますか。ベンダーは、この情報を受けてどのような行動を取りますか。ベンダーには脆弱性管理プロセスがありますか。	• 脆弱性は、どの製品やコンポーネントからも見つかる可能性があります。責任ある企業は、自社製品に脆弱性が見つかった場合には、適切なタイミングで必ず公表すべきです。 • ベンダーは、いかなる脆弱性情報にも対処できなければならず、したがって誰から問題の報告を受けたかにかかわらず、脆弱性管理に対するエンド・ツー・エンドのプロセスを実証できなくてはなりません。
66. ベンダーは、サプライヤーのいずれかがサイバー・セキュリティ要件に従っていない、従いそうにない、あるいは従うことができない場合、どのようなアプローチを取りますか。	• サイバー・セキュリティ要件への準拠には明らかにコストが伴う一方、メリットは目に見える直接的なものではない場合があります。 • ベンダーのサプライヤーが所定のサイバー・セキュリティ要件に従わない場合、ベンダーは、サイバー・セキュリティの課題に一緒に取り組むようサプライヤーに促すために、どのような手段を講じますか。それでも従わない場合には、どのような対策を取りますか。

要件	さらなる考慮事項
67. ベンダーは、C-TPAT（Customs-Trade Partnership Against Terrorism：テロ行為防止のための税関・産業界パートナーシップ）や TAPA（Transported Asset Protection Association：輸送資産保全協会）の標準のような、国際的なベスト・プラクティスの標準に従っていますか。また、認証を取得していますか。	• どの標準が最も優れているかについては世界各地でさまざまな見解があるかもしれませんが、ベンダーは広く受け入れられている標準に準拠していることやそれに基づいた認証を受けていることを実証できなくてはなりません。 • 標準は必ずしも完全ではないという認識があるかもしれませんが、ベンダーは自分たちが標準を上回るプラスアルファの保護や対策を提供できる領域を示せなければなりません。
68. ベンダーは、サプライヤーのセキュリティに関して現地監査を実施していますか。そうした監査の対象範囲はどこまでですか。ベンダーは、サプライヤーと協力して、監査で見つかった問題をどのように解決していますか。	• どのベンダーやサプライヤーも、それぞれのお客様のニーズに注力する必要があります。監査および検査により、サプライヤーの焦点が明確になり、要件の実現も保証されます。相互のニーズを知るための協調的アプローチは、パフォーマンスを適切な方向に導きます。

4.8 製　造

製品の製造業者は、さまざまなサプライヤーからコンポーネントを調達しなければならず、そのため生産プロセスのすべての段階を通して、セキュリティ・リスクが入り込んでいないことを保証しなければなりません。

要件	さらなる考慮事項
69. 製造に関して、ベンダーはどの国際標準やベスト・プラクティスに準拠していますか。	• 製造拠点には数多くの複雑なプロセスや作業があり、品質から環境に至るまでの数々の標準で幅広くカバーされています。ベンダーは、製造プロセスに対して最高の国際標準とアプローチを採用する総体的な取り組みをどのように行っているのかを実証できなければなりません。
70. ベンダーの製造プロセスの流れはどのようなものですか。また、開始時点と終了時点の双方においてどのようにしてプロセスを評価して、不良製品や偽造製品を見つけ出していますか。	• 製造プロセス内には、部品がベンダーの製造拠点に到着する前や、製品が組み立てられてお客様の元へ発送された後も含めて、コンポーネント不良が発生する恐れのある工程が数多くあります。ベンダーは、世界各地で部品交換や返品をどのように取り扱っているのかを詳しく説明できる必要があります。とりわけ考慮すべきなのは、お客様の個人データが含まれている場合があるストレージ・メディアの取り扱いです。
71. ベンダーは、サプライヤーから購入したコンポーネントが、製造拠点に届いたコンポーネントと一致していること、期待どおりのものであることをどのようにして確認していますか。	• 不良品の可能性がある高性能なコンポーネントは、セキュリティ上の危険にさらされている場合があります。したがって、「何でも信用する」のではなく、「何も信用しない」という姿勢で臨むべきです。ベンダーはどのようなアプローチを取っていますか。
72. ベンダーは、いかなるコンポーネントも、製造拠点内で自社のスタッフによって手を加えられることが絶対にないようにするために、どのような対策を講じていますか。	• 内部脅威の問題は現実に存在します。ベンダーは、納入資材を検証してその完全性を確認する必要があるのと同様に、製造拠点から出荷する商品が自社のスタッフによって手を加えられていないことを保証するプロセスと管理方法も実証できなければなりません。

要件	さらなる考慮事項
73. ベンダーは、出荷前の完成品に対して、どのような不正開封防止対策を講じていますか。	• 出荷を待つ完成品は、不正に手を加えやすい状態にあります。ベンダーは、自社の工場や倉庫において、どのようにしてこうした行為から製品を守っていますか。
74. ベンダーは、お客様が受け取る製品が、ベンダーの製造拠点から出荷された製品と同じものであることをどのようにして保証していますか。	• 製品の出荷後、ベンダーは工場から安全でセキュアな状態で出荷された製品がお客様の手元に届く前に手を加えられる可能性を考慮しなければなりません。物流管理会社を選ぶ際には、物流管理を取り巻く包括的プロセスを評価して検討すべきです。
75. ベンダーは、できるだけ頻繁に最新のコンポーネントを調達できるように、どのようにしてコンポーネントの需要計画を立てていますか。	• 脆弱性はいつでも見つかり得ることを考えると、過剰供給は、脆弱性が含まれたコンポーネントを在庫することにつながりかねません。ジャスト・イン・タイムの製造を行うことで、このリスクが軽減されます。これを効果的に行うには、売上予測を包括的に計画し、それが自動的に製造とリンクするようにしておかなければなりません。
76. お客様固有のソフトウェアが最終機器に搭載される場合、ベンダーはそれが研究開発チームから許可されたものと同じソフトウェアで、何も手を加えられていないことを、どのようにして保証していますか。	• ベンダーは、エンド・ツー・エンドのインテグレーションを実行し、ハードウェアとソフトウェアが 1 つの場所で 1 つのプロセスを完了してから別の場所で別のプロセスに入るまでの間に、他者が手を加える隙や機会がないということを示せなければなりません。
77. ベンダーは、製造拠点のスタッフが製品にマルウェアをロードできないことをどのようにして保証していますか。	• 製造では、ソフトウェアの保護が非常に重要です。ベンダーは、このプロセスがどのように制限されているかを実証できるとともに、これを受け持つ役職を「重要」に分類し、内部脅威のリスクを回避するための特別な監視対象としているかどうかを詳しく説明できなければなりません。
78. ベンダーの製造拠点内では、製品の出荷時に初期設定ですべてのテスト・ポートが閉じられ、製造拠点を出た後には誰もアクセスできないことをどのようにして保証していますか。	• 製造施設では、製品のテスト・ポートへのアクセスが必要になることが頻繁にあります。それらがしっかりと管理されておらず、製造の完了時に開いたままになっていると、設置時にハッカーに悪用の機会を与えてしまう場合があります。ベンダーは、体系的な製造工程の一環として、すべてのテスト・ポートがどのように自動的に閉じられるのかを実証できなければなりません。
79. 製造工程では、特定のお客様の機器に手を加えることができないよう、機器の納入先がどのお客様なのかが権限を持つ人以外には絶対にわからないようにするために、ベンダーはどのような対策を講じていますか。	• 製造拠点における脅威というのは特定の製品が対象になる可能性が高いですが、賄賂や悪意によって特定のお客様の機器が狙われる状況も万全の対策を講じて回避しなければなりません。ベンダーは、どの特定の機器がどのお客様に納入されるのかを知る人々を制限すべきです。お客様の名前ではなく、コーディング規約の使用などの手法を用いるようにします。
80. 過剰注文や契約のキャンセルのために、お客様から「未使用」の状態で製品が返品されてきたとき、ベンダーは返品の前に製品に手を加えられていないことをどのようにして保証していますか。	• ベンダーは、たとえ製品が返品されてきた場合でも、やはり「何も信用しない」というアプローチを取るべきです。製品に不良や破損が生じていることを前提として手順やプロセスを設定し、製品の完全性を再検証する必要があります。
81. 欠陥のある製品が返品されてくる場合、それが返品センターに送られる前に、ディスクやストレージからお客様のデータが完全に消去されていることを保証するために、ベンダーはどのようなプロセスを整備していますか。	• テクノロジー機器には通常、ストレージ・コンポーネントが組み込まれています。したがって、何らかのエラーや欠陥のために返品されてきた製品には、お客様のデータが含まれている場合があります。ベンダーは、データ保護に関する各地の法律を認識しておかなければなりません。 • ベンダーは、自社の返品およびスクラップ・プロセスがどのように機能しており、ストレージ・メディアにアクセスしてデータの完全消去を行うことができない場合にはどのように対処しているかを示せなければなりません。

要件	さらなる考慮事項
82. 欠陥のある製品がベンダーの修理センターで修理された場合、交換可能ユニットがすべてオリジナルである（すなわち、偽物と交換されていない）ことと、製品にマルウェアが組み込まれていないことを、ベンダーはどのように保証していますか。ベンダーはこうした製品の再テストを行っていますか。	• ベンダーは、「何も信用しない」というアプローチを取らなければなりません。弱点は、プロセスのさまざまな段階で入り込む可能性があるのです。製品の修理や再配送が行われる場合、ベンダーは、不正に手を加えられたコンポーネントの侵入、偽造ユニットの使用、マルウェア、誤設定のリスクをどのように軽減させているかを示すべきです。 • 欠陥のある製品の再検証を行うことで、不正に手を加えられた製品、不正な組み込みが行われた製品や、偽造製品が、欠陥部品の返品プロセスを通じてサプライチェーンに入り込むのを防ぐことができます。
83. ベンダーには、コンポーネントに対するトレーサビリティ機能やプロセスがありますか。問題というのは、ベンダーのハードウェアやソフトウェアの中や、ベンダーのスタッフから、あるいはサードパーティからというように、どこからでも生じる可能性があります。問題が発生した場合に、ベンダーはその問題に関連する「誰が」「何を」「なぜ」「いつ」「どこで」を、どのようにしてトレースすることができますか。	• 正確かつ迅速なトレーサビリティ・システムがあると、問題の発生源を迅速に突き止めて問題の範囲を見極めることが可能となり、ベンダーは、問題の拡大を防ぐための措置を取るよう関係各位に通知することができます。 • 前方・後方の双方にトレースができれば、ベンダーが問題の根本的原因を特定し、実行可能な改善点を見極め、将来的に同じ問題が発生することを防ぐのにも役立ちます。

4.9 安全なサービス・デリバリー

製品の設計段階でセキュリティをどれほど考慮しても、設置やサポートの段階を安全に遂行しなければ意味がありません。お客様は当然ながら、自社の事業を支える装置に対する運用保守が安全で安心できるものであることを望んでいます。

要件	さらなる考慮事項
84. ベンダーのサービス・エンジニアは、設置後に運用されているお客様の機器やサービスに対して、どのようなアクセスを必要としていますか。彼らは必要なときに必要なものにアクセスできますか。	• ベンダーは、お客様の技術やサービスに対する第三者のアクセスはお客様自身が常に制御できるということを示さなければなりません。そのため、ベンダーは、自分たちに何ができて何ができないかということに関して、自社のスタッフの行動を規制し責任を明確にするさまざまなプロセスや指針を持っている必要があります。 • お客様は多くの場合「書面による明確な許可」を必要とすることを原則とし、指針が守られているかどうかを確認するために設備の監査を要求します。
85. ベンダーは、システムのデフォルトのアカウントや、サポート・保守サービスを請け負うためにお客様から許可を受けたアクセス用アカウントを、どのようにして保護していますか。	• ベンダーは、その指針や手順の一環として、これらのアクセス権限がどのように利用されるのか、どのように保護されるのか、いつ返還されるのかということと、これらが独立した検証や監査の対象になり得るということを示さなければなりません。

要件	さらなる考慮事項
86. ベンダーは、自社のエンジニアが携行しているノート・パソコンやエンジニアリング技術の使用に関して、どのようなガイドラインを設けていますか。例えば、ベンダーのエンジニアは、自分のラップトップに独自のソフトウェア・ツールをインストールすることができますか。	• もし従業員のノート・パソコンがハッキングされたり、マルウェアに感染したりしたら、悪意のある行為者がそれを通じてお客様情報を盗み出したり、お客様のネットワークを攻撃したりすることができてしまいます。したがってベンダーは、従業員のノート・パソコンの保護と監視のためにどのような対策を講じているかを詳しく説明すべきです。
87. ベンダーは、従業員がそれぞれのお客様に対して適切なソフトウェアしか使用しないようにするために、どのようなプロセスと制御手段を整備していますか。	• 多くの場合、お客様の技術は複雑で、そこにはさまざまなベンダーの技術が組み込まれており、そうした複数のコンポーネントを効率よく連動させるために特別なソフトウェアが必要になることもあります。ベンダーは、お客様の技術に対して行う変更やアップグレードはすべて、バージョンやリリース・レベルが正しいかどうかを含め、お客様が承認するソフトウェアと一致していることを実証できなくてはなりません。
88. ベンダーは、自社のサービス・エンジニアやサポート・エンジニアが、インストール済みのソフトウェアに不正に手を加えたり、脆弱なソフトウェアや悪意のあるソフトウェアをインストールしたりすることを確実に防止するために、どのような対策を講じていますか。	• サポート・エンジニアが悪意や過失によりお客様が要求していないものを残していないかどうかを知る必要があります。そうしたものが残されていると、悪意のある攻撃者がハードウェア・コンポーネントを入れ替えたり未承認ソフトウェアをインストールしたりして製品の完全性を損なわせ、悪意のあるソフトウェアや脆弱なソフトウェアを組み込むことが可能になるからです。 • ベンダーは、「何も信用しない」というアプローチにより、ソフトウェアの配備やアップグレードのプロセスにおいて悪意のある攻撃者が製品やコンポーネントに不正に手を加えることをどのように防いでいるかを実証できなければなりません。
89. ベンダーは、それぞれのお客様に特化したハードウェアの堅牢化、ソフトウェアおよびハードウェアのチェック、セキュリティ製品（ファイアウォールなど）に対してどのようなアプローチを取っていますか。	• ベンダーや自社の ICT チームが購入する機器の「堅牢化」（攻撃耐性の強化）を行う際にガイドラインとなるような文書化されたベスト・プラクティスはたくさんあります。また、購入する機器にさまざまなセキュリティ対策やセキュリティ機能が組み込まれている場合もあります。 • インストール、サポート、保守に関するあらゆる活動をこうしたベスト・プラクティスに従うようにし、関連する設備の電源のオン／オフも適切に行われるよう確認する必要があります。
90. ベンダーは、トラブルシューティングのためにデータの取得が必要になった場合、お客様の正式な許可を得てから、その権限の範囲内でのみデータ取得を行っていますか。また、どのようにして取得したデータを管理し、個人データを保護していますか。	• テクノロジー機器のトラブルシューティングを行うには、機器上のデータへのアクセスが必要になることがあります。ユーザーの個人データやビジネスに関するデータが必要となる場合、それらが確実に保護されるよう、合意に基づく指針と手順がなければなりません。
91. ベンダーは、自社のサポート・エンジニアが現場で問題を解決できず、取得したデータを別の国に送ってレビューしてもらう必要が生じた場合、お客様の要件と現地の法律に対するコンプライアンスを保証するために、どのようにしてそれを管理しますか。	• 発生した障害が複雑すぎて、現場のエンジニアが修理できないことがあります。その場合、別の拠点にいる研究開発エンジニアがトラブルシューティングを行わなければなりません。 • ベンダーとお客様は、必要とされるサポートが国内では提供されていない場合などのデータの取り扱い方について合意しておく必要があります。ベンダーは、こうした状況にどれぐらいの柔軟性を持って対応していますか。

要件	さらなる考慮事項
92. ベンダーは、トラブルシューティングのために取得したデータが不要になった場合、そのデータをどのようなプロセスで取り扱っていますか。	• データはお客様の資産であり、許可された正当な範囲内でのみそれを使用することができます。サービスが終了したときには、そのサービス以外の目的でデータが使用されるのを防ぐために、データを消去しなければなりません。ベンダーは、どのようにしてこれを行い、またその徹底に努めていますか。
93. 監査ログは、システムで何が行われているかを証明する重要なものです。ベンダーは、自社の監査ログに関連情報がすべて含まれていることをどのように保証していますか。	• ベンダーは、正確な監査ログの記録と保護のためにどのようなアプローチを取っているかを示せなくてはなりません。 • 業界で広く認知され使用されている監査ソフトウェアを利用していれば、より客観的で信頼性の高い結果を得ることができます。
94. お客様は、とりわけサービス断や自然災害などの危機の際、事業継続のためにベンダーを頼りにします。ベンダーには、困難な状況に陥ったときのお客様へのサポートに対して、どれだけの準備と意欲がありますか。実例を尋ねてみてください。	• ベンダーはお客様とサイバー・セキュリティの要件やロードマップ、計画について議論する恒常的な窓口を持ち、お客様のサイバー・セキュリティ戦略を危機発生時を含めて最大限満たすことができますか。 • 脅威の実行者はあらゆる機会に乗じるため、コンピューター・ユーザーに対するリスクはいつでも、大災害のときでさえ襲ってきます。多くのベンダーは、お客様に役立つ国際的な知識、ツール、リソースを豊富に持っています。例えば、頻繁なサービス妨害攻撃に対しては、新しい技術や異なる技術による迅速な機器拡張が必要になる場合がありますが、ベンダーにはそうした状況で支援への意欲と柔軟性を示してもらいたいものです。 • 自然災害というのは必ず起こるものであり、組織の事業継続においてベンダーが重要な役割を果たす可能性があります。こうした困難な状況下での支援にどれだけ意欲があるかを探ってみると、お客様のビジネスの成功に対するベンダーの長期的なコミットメントを評価することができるでしょう。

4.10 問題、障害、脆弱性の解決

セキュリティを 100% 保証することは不可能です。そのため、問題に効果的に対処し、失敗に学ぶ能力が、お客様とベンダー両者にとって非常に重要となります。

要件	さらなる考慮事項
95. ベンダーには、PSIRT（Product Security Incident Response Team：製品セキュリティ・インシデント対応チーム）／ベンダー CSIRT（Computer Security Incident Response Team：コンピューター・セキュリティ・インシデント対応チーム）、またはそれと同等のチームがありますか。ベンダーはどのような業務体制を取り、どのような連絡方法を持っていますか。PSIRT ／ベンダー CSIRT チームが従わなければならないプロセスと要件はどのようなものですか。	• 問題は起きるものであり、それが起きたときに実際の、あるいは疑われるセキュリティ上の問題をベンダーがすばやく把握できるかどうかを知っておく必要があります。また、セキュリティ・インシデントを解決されるまで追跡できるメカニズムも整備しておいたほうがいいでしょう。 • PSIRT ／ベンダー CSIRT チームが責務の遂行において従うべきプロセスを承認しておくことが重要です。

要件	さらなる考慮事項
96. ベンダーは、お客様の CSIRT やコーディネーターがベンダーに問題を報告し、互いに協力して迅速にその問題に取り組めるようにするために、どのようなメカニズムを整備していますか。	• 社内の 1 つの中枢（PSIRT ／ベンダー CSIRT）から複数の場所へと伝達できる多様な連絡メカニズムがあったほうがいいでしょう。ベンダーは、さまざまな方法を採用できる能力と柔軟性を持っていなければなりません。
97. ベンダーは、セキュリティ研究者コミュニティと協力しようとしていますか。	• 人の言葉に耳を傾けない組織は学習しません。ベンダーは、自分たちの製品に問題点を見つけているかもしれないさまざまな企業や個人と協力する必要があります。ベンダーは、どのようにしてこうした協力を生産的かつ専門的な形で行っていますか。
98. ベンダーは、大規模なインシデントが発生した際にお客様に適時に情報を伝え、インシデントに対応するためのリソースを社内で適切に用意するための準備をどれだけ整えていますか。ベンダーのエスカレーション・プロセスはどうなっていますか。	• お客様の組織内で重大なインシデントが発生した場合、ベンダーはそれをお客様に迅速に通知するメカニズムを持っている必要があります。また、ベンダーの組織内でのエスカレーションを含め、ベンダー側にも社内のインシデント対処プロセスがなければなりません。 • ほとんどの企業では、熟練した人材が何もせずにただじっと座って待っているわけではありません。ベンダーは、自社の上級役員がこうした状況を当然のこととして認識していて、問題解決のために必要なサポートをいつでも割り当てられるようにしているということを示せなくてはなりません。

4.11 監　査

口で言うだけなら簡単で、言っていることは立派かもしれません。しかし、約束したことを、約束した方法で、約束した時間、コスト、品質、セキュリティ要件を満たしながら、本当に実行できるのでしょうか。セキュリティに関する適切な方針、手順、標準が実施され、要求された成果を達成したことをお客様やステークホルダーに対して証明するうえで、厳格な監査は重要な役割を担っています。

要件	さらなる考慮事項
99. 関連する取締役会委員会が、単に報告を聞くだけでなく、組織の実際のリスク状況やインシデントの状態や結果をじかに把握できるよう、ベンダーはどのような社内セキュリティ監査・報告のプロセスとメカニズムを整備していますか。	• サイバー･セキュリティに関する活動に対して､社内監査人､社外監査人､お客様､サードパーティによる正式な監査が行われている場合には、取締役会が実際のフィードバックに対してオープンであるということです。 • これを実証できるということは、戦略、指針、標準が「生きて」いて、新たな脅威や状況に順応していることを示しています。 • サイバー・セキュリティに関する活動とその進捗状況や成果について、正式な報告が取締役会や委員会に提出されていれば、それが「プロジェクト」や何らかの「特別な」イベントではなく、通常のビジネス活動の一部になっているということです。
100. ベンダーには、社外のステークホルダーやそこから委託された組織による監査の実施を認めるメカニズムがありますか。	• 主要なステークホルダーに対してオープンで透明性の高い姿勢を持ち、社外からの監査や評価を受け入れていれば、高いコミットメントと継続的学習の文化があることになります。 • 社外グループによる評価にオープンであるほど、改善に向けた提言をより多く得ることができます。

5　ファーウェイについて

ファーウェイは、170 か国以上で事業を運営し、世界人口の 3 分の 1 以上にも及ぶ人々に製品とソリューションを提供しています。15 万人の従業員を擁し、その平均年齢は 32 歳で、各国の従業員の平均 79% が現地採用です。2013 年末までに、281 の LTE 商用契約と 162 の EPC（Evolved Packet Core：進化型パケット・コア）商用契約を締結し、そのうち 110 の LTE ネットワークと 88 の EPC ネットワークが商用化を開始しています。

当社は継続的なイノベーションを通じて通信業界を牽引し、業界屈指の IPR ポートフォリオを誇っています。また、他者の IPR を尊重し、その保護に努めています。売上の 10% 以上を R&D に投資しており、従業員の 45% が R&D に従事しています。2013 年は年間総売上高の 12.9% にあたる 306 億 7,200 万人民元（約 5,309 億円[3]）を R&D に投資し、過去 10 年間で総額 1,510 億人民元（約 2 兆 6,138 億円[3]）を R&D 費に充ててきました。

2013 年 12 月 31 日までのファーウェイの申請済み特許件数は中国国内で 4 万 4,168 件、中国国外で 1 万 8,791 件、PCT（Patent Cooperation Treaty：特許協力条約）に基づくものが 1 万 4,555 件です。取得済みの特許ライセンスは累計で 3 万 6,511 件に上ります。当社では、IPR の数よりも商業的価値と品質により重点を置いています。2010 年から現在までに、当社が 3GPP に提案した LTE コア技術に関する提案のうち 466 件が承認されており、その数は業界最多となっています。ファーウェイは、FTTP（Fibre To The Premises：ユーザーの敷地内まで光ケーブルを引き込むネットワーク構成方式）、OTN（Optical Transport Network：光伝送ネットワーク）、G.711.1（固定ブロードバンド音声コーデック）などの特許において主導的な立場にあります。IPR の保護はファーウェイの継続的な成功にとって不可欠であり、当社は IPR 保護の重要性を積極的に提唱しています。

ファーウェイは全世界で 16 か所の研究機関、28 か所の共同イノベーション・センター、45 か所のトレーニング・センターを有しています。売上の 65% は中国国外からのものであり、資材の 70% は外国企業から調達しています。米国は最大の供給元で、米国からの部品は全体の 32% を占め、2013 年は米国の企業から 72 億 3,700 万米ドル（約 7,589 億 4,419 万円[4]）を購入しました。

ファーウェイは 75 か国の 120 を超える通信事業者にマネージド・サービスを提供し、お客様が優れた運用ができるよう支援しており、累積で 340 を超える契約を締結しています。また、クラウド・ベースの IT ソリューションを構築し、400 以上のパートナーと共同で、さまざまな業界でクラウド・コンピューティング技術の商用利用を推進してきました。2013 年末までに、当社はお客様のために世界中で 330 のデータセンターを構築しており、そのうち 70 か所がクラウド・コンピューティング・データセンターです。

2013 年度のファーウェイのコンシューマー向け端末事業の全世界での製品出荷台数は 1 億 2,800 万台で、その内訳は、携帯電話が 6,000 万台近く、モバイル・ブロードバンド端末が 4,450 万台、ホーム・デバイスが 2,440 万台です。スマートフォンのコンシューマー向け出荷台数は前年比 60% 超の 5,200 万台に達しました。

ファーウェイは主要な国際標準を積極的に支持し、その策定に貢献しています。2013 年末までに、3GPP、IETF、ITU、OMA、ETSI、TMF、ATIS、オープン・グループなど 170 以上の標準化団体に参加し、2013 年には 5,000 件を超える提案を提出するとともに、185 以上の役職に就き、国際標準に対する合意の促進に尽力しています。

ファーウェイの株式は 2013 年 12 月 31 日時点で 8 万 4,187 人の従業員が保有しています。当社の従業員持株制度は、会社の長期的な発展と従業員の個人的な貢献とを密接に結びつけ、長期にわたる献身と共有を可能にする仕組みです。この制度によって、当社は長期的な視野を持ち、リスクに対する利益と戦略のバランスを取ることができます。従業員は、お客様に優れたサービスを提供できなかったり、不適切な行動を取ったりすれば、自らの資産が損なわれることを理解しています。

[3] 1 人民元あたり 17.31 円で換算（2013 年 12 月 31 日現在）
[4] 1 米ドルあたり 104.87 円で換算（2013 年 12 月 31 日現在）

Copyright © 2014 Huawei Technology Co., Ltd. All rights reserved.

本レポートは内部参考資料としてのみ印刷・利用できます。それ以外の目的に使用することはできません。

本レポートは「現状のまま」にて提供され、明示または黙示を問わず、一切の保証を伴いません。すべての保証は明示的に放棄されます。権利非侵害、商品性、特定の目的への適合性に対する保証は一切ありません。ファーウェイは内容の正確さについて一切の責任を負いません。本レポートに記載されたすべての情報は予告なく訂正・修正・変更されることがあります。本レポートの内容を信頼し、利用するにあたってその責任はすべて利用者に帰されます。本レポートに記載された第三者に関する情報は公共の情報源または公開された報告や説明に基づいたものです。

HUAWEI、 はファーウェイ・テクノロジーズの商標または登録商標です。

本レポートで言及されるすべての企業名・商標は該当する各社の商標または登録商標です。

VEGETABLE OIL INK この提言レポートは再生紙を使用しています